IN THE UNITED STATES DISTRICT COURT DISTRICT OF UTAH	
IN THE MATTER OF THE SEARCH OF A TCL T779 CELLPHONE BEARING IMEI 016099001432453 IN THE POSSESSION OF KEVIN WILLIAM PETERSEN	Case No. 2:24mj195 CMR AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT Judge Cecilia M. Romero

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jeffrey Chmielewski, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent ("SA") with Homeland Security Investigations ("HSI"), assigned to the HSI Salt Lake City, Utah, office. I am concurrently assigned to the Utah Internet Crimes Against Children ("ICAC") Task Force, managed by the Utah Attorney General's Office, and the Child Exploitation Task Force ("CETF"), managed by the Salt Lake City Federal Bureau of Investigation ("FBI"). Prior to being employed by HSI, I was a Colorado State Patrol Trooper for approximately six years. My formal law enforcement training includes completing the Criminal Investigator Training Basic training course and the HSI Special Agent Training program at the Federal Law Enforcement Training Center in Glynco, Georgia. I have received additional training from CETF, ICAC, and other sources related to Child Sexual Abuse Material ("CSAM"), to include child pornography (as defined in 18 U.S.C. § 2256), and exploitation investigations and specifically to online, undercover enticement.

2. I have been involved in investigations of federal criminal violations, including those related to the distribution, receipt, and possession of CSAM, child enticement and exploitation, and cybercrime. I have reviewed numerous examples of CSAM. I have become familiar with ways that CSAM is shared, stored, distributed, and/or produced, including the use of various social media websites (Facebook, Instagram, Twitter, Kik, Snapchat, Discord, etc.), messaging platforms and applications, electronic media storage, "cloud" based storage, and peer-to-peer ("P2P") networks. I have also become familiar with jargon or slang terms that people involved in child exploitation use to discuss their activities. I have gathered evidence pursuant to search warrants and have participated in searches of premises, persons, and electronic devices. I have conversed in undercover, online conversations with, and upon arrest, have interviewed persons who possess, view, and distribute CSAM or who seek to commit physical sexual offenses against minors.

3. As a federal agent, I am authorized to investigate violations of laws of the United States, and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of a residence described in Attachment A.

PURPOSE OF THE AFFIDAVIT

4. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41(b)(1) to search a cellular telephone (the "SUBJECT CELLPHONE") of KEVIN WILLIAM PETERSEN ("PETERSEN") more fully described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C.

§ 2422(b) (online enticement of a minor), 18 U.S.C. §§ 2252(a)(1) and (2) and 2252A(a)(2) (Transportation/Receipt/Distribution of Child Pornography), and 18 U.S.C. §§ 2252(a)(4) and 2252A(a)(5)(B) (Possession of Child Pornography), the SUBJECT OFFENSES committed by PETERSEN as described in Attachment B hereto.

5. The statements in this affidavit are based upon my personal observations, my training and experience, and information provided by law enforcement officers assigned to other law enforcement agencies, and other special agents. This affidavit is being submitted for the limited purpose of securing a search warrant and intended to show merely that there is sufficient probable cause for the requested warrant. Thus, I have not included each and every fact known to me concerning this investigation.

BRIEF SUMMARY

6. On October 8, 2021, PETERSEN was sentenced in the State of Utah for Sexual Exploitation of a Minor to felony probation for approximately 16 months and was re-added to the Utah Department of Corrections ("UDC") Sex Offender Registry. PETERSEN has a consistent history of sex offense charges and convictions since 2008.

7. As a condition of his felony probation, PETERSEN was subject to a Probation Agreement by the UDC Adult Probation and Parole ("AP&P") relating to probation visits, probation reporting, conduct, searches, and truthfulness among others. As another term of probation, PETERSEN was also a restricted internet user and did not have permission from AP&P to access the internet. In February 2023, PETERSEN reported to the Utah Department of Corrections Adult Probation and Parole Office in West Valley City, UT for routine classes. PETERSEN was subsequently advised that he would be arrested pursuant to an active arrest

warrant that had been issued by a Utah State judge on an unrelated matter. When PETERSEN was informed he would be arrested, PETERSEN stated he had items on his person that he could not take into the jail. PETERSEN then produced drugs and drug paraphernalia from his bra. Possession of these items was a violation of the terms of his probation. PETERSEN was then searched pursuant to his arrest. Also on his person at the time of arrest was the SUBJECT CELLPHONE, with access to the internet. Possession of this device was another violation of the terms of PETERSEN's probation. A cursory review of the phone by AP&P agents pursuant to AP&P search authority identified several messaging and social media applications, images pertaining to "Adult Baby/Diaper Lover," and images of toddlers in diapers.

JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is "a district court of the United States … that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

DEFINITIONS

9. Based on my training and experience, I use the following terms to convey the following meanings:

a. "Chat" is any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

c. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Internet Service Providers" are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

h. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

i. "Mobile application" or "chat application" is a small, specialized program downloaded onto mobile devices, computers and other digital devices that enable users to

perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

j. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic digital media.

k. "Remote computing service" is defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

l. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality;

(c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

m. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disk or other electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON COMPUTERS AND CSAM (CHILD PORNOGRAPHY)

10. Based on my knowledge, training, and experience in child exploitation and CSAM investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers, computer technology, and the Internet have drastically changed how CSAM is produced and distributed.

11. Computers serve four basic functions in connection with CSAM: production, storage, communication, and distribution.

12. Child pornographers can upload images or video clips directly from a digital camera to a computer. Once uploaded, they can easily be edited, manipulated, copied, and distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer using a scanner. Once uploaded, they too can easily be edited, manipulated, copied, and distributed. A modem allows any computer to connect to another computer via a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

13. The computer's ability to store images in digital form makes it an ideal repository

for CSAM. The size of the electronic storage media (commonly referred to as the hard drive or more recently, memory) used in home computers has grown tremendously in the last several years. This storage can store millions of images at very high resolution. Images and videos of CSAM can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like, many of which are small, highly portable, and easily concealed, including on someone's person or inside their vehicle.

14. The Internet affords collectors of CSAM several different venues for obtaining, viewing, and trading CSAM in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs such as Kik, bulletin board services, e-mail, "peer-to-peer" (P2P) file sharing programs such as LimeWire and eMule, and networks such as eDonkey, Gnutella, ARES, Tumblr, and BitTorrent. Collectors and distributors of CSAM sometimes also use online resources such as "cloud" storage services to store and retrieve CSAM. Such online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet and can access stored files using any device capable of connecting to the Internet. Evidence of such online storage of CSAM is often found on the user's computer.

15. An Internet Protocol (IP) address is a unique identifier that electronic devices such as computers, routers, fax machines, printers, and the like use to identify and communicate with each other over a network. An IP address can be thought of as a street address. Just as a street address identifies a particular building, an IP address identifies a particular Internet or network access device. When a user logs on to his/her Internet Service Provider (ISP), they are assigned an

IP address for the purpose of communication over the network. An IP address can be statically assigned, meaning the IP address does not change from one Internet session to another, or dynamically assigned, meaning a user receives a different IP address each time the user accesses the Internet. An IP address can only be assigned to one user at a time, and ISPs keep records of who IP addresses are assigned to by date and time. Similarly, cell phone service providers also generally keep IP records that can identify what device (cell phone) utilized the IP address on a certain date and time.

16. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in the computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

17. I know, based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including persons who collect and trade in CSAM, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such

persons maintain their collections of CSAM in safe, secure, and private locations, such as their residence or vehicle, and on computers and digital storage media under their direct control. Such persons often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period. In some cases, however, persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of CSAM indefinitely.

18. I also know from my training and experience that many people who download CSAM from the Internet, and those who collect CSAM, frequently save images and videos of CSAM on their computers and/or transfer copies to other computers and storage media, including cloud storage accounts, external hard drives, thumb drives, flash drives, SD cards, and CDs or DVDs. Moreover, it is common in child exploitation investigations to find CSAM on multiple devices and/or storage media located in suspects' homes, rather than on a single device.

19. I know based on my training and experience that many social media and messaging platforms, such as Facebook, Instagram, Twitter, Signal, Snapchat, Kik messenger, and others can be directly accessed and used with one's cellular phone. Often, these applications require the user to download the application directly to their phone, which then allows seamless use between the cellular phone and the social media or messaging website.

BACKGROUND ON THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN (NCMEC) AND CYBERTIPLINE REPORTS

20. The National Center for Missing and Exploited Children (NCMEC) is a private, non-profit organization established in 1984 by the United States Congress. Primarily funded by the Department of Justice, the NCMEC acts as an information clearinghouse and resource for parents,

children, law enforcement agencies, schools, and communities to assist in locating missing children and to raise public awareness about ways to prevent child abduction, child sexual abuse and depictions of minors engaged in sexually explicit conduct.

21. The NCMEC CyberTipline offers a means of reporting incidents of child sexual exploitation, including the possession, manufacture, and/or distribution of depictions of minors engaged in sexually explicit conduct; online enticement; child prostitution; child sex tourism; extra familial child sexual molestation; unsolicited obscene material sent to a child; and misleading domain names, words, or digital images.

22. Federal law requires NCMEC to operate the CyberTipline and requires Electronic Service Providers ("ESPs") to report apparent instances of child pornography offenses. Providers also have the discretion to submit reports concerning planned or imminent child pornography offenses. Companies that suspect child pornography has been stored or transmitted on their systems report that information to NCMEC in a CyberTipline Report (or "CyberTip"). The ESP submits the report, which generally contains account and log-in information, and uploads content to NCMEC via a secure connection. Aside from required information such as incident type, date, and time, reporters can also fill in voluntary reporting fields such as user or account information, IP addresses, or information regarding the uploaded content itself, as well as other information it may have collected in connection with the suspected criminal activity. The ESP may or may not independently view the content of the file(s) it uploads. Using publicly available search tools, NCMEC then attempts to locate where the activity occurred based on the information the ESP submits, such as IP addresses. NCMEC then packages the information from the ESP along with any additional information it has, such as previous related CyberTips, and sends it to law

enforcement in the jurisdiction where the activity is believed to have occurred.

STATEMENT OF PROBABLE CAUSE

A. PETERSEN is Arrested and is Convicted of Sexual Exploitation of a Minor

23. PETERSEN has a consistent history of sex offense charges and convictions since 2008. PETERSEN was arrested for an unspecified sex offense by the Unified Police Department of Greater Salt Lake in 2008. In October of 2009, PETERSEN was charged in the State of Utah with failing to register as a sex offender and with being a sex offender in presence of a child. In 2016, PETERSEN was again charged in the State of Utah with failing to register as a sex offender.

24. In 2021, under investigation by the Utah Attorney General's ("AG's") Office, PETERSEN was charged with and convicted of Sexual Exploitation of a Minor in the State of Utah. In an interview pursuant to this investigation, PETERSEN told investigators that he only deals in (including uploading) child pornography when he is "super-high," and that his drug of choice is methamphetamine.

25. On October 8, 2021, PETERSEN was sentenced in the State of Utah for Sexual Exploitation of a Minor to felony probation for 48 months and was again added to the UDC Sex Offender Registry. According to several record sources including the AG's Office report and the Sex Offender Registry, PETERSEN is known to use several aliases including Eden Delmar and Eden PETERSEN.

B. PETERSEN is Found with an Internet Accessible Cellphone in Violation of his Probation Agreement

26. As a condition of his felony probation, PETERSEN was subject to a series of probation agreements by AP&P relating to probation visits, probation reporting, conduct, searches,

and truthfulness, among others. PETERSEN signed his AP&P Probation Agreement on March 2, 2022. This agreement specifies the conditions of his probation, including allowing AP&P agents to search his person, residence, vehicle, or any other property at any time upon reasonable suspicion of violations of the terms of probation. Special conditions of the Probation Agreement include the full restriction of internet access as a sex offender, a restriction against contacting the victim(s) or victim's family, restrictions against access to children or areas where children congregate, restrictions against the possession of sexually exploitatively material, a requirement to complete sex offender classes and therapy, and restrictions against drug and alcohol use or access, among others.

27. Per PETERSEN's Probation Agreement, PETERSEN was also a restricted internet user and did not have permission from AP&P to access the internet.

28. In February 2023, PETERSEN reported to the AP&P Office in West Valley City, UT for routine classes. PETERSEN was subsequently advised that he would be arrested pursuant to an active arrest warrant issued by a Utah State judge in an unrelated matter.

29. PETERSEN informed AP&P Agent Ashley Powell that he had items on his person that could not take to the jail. Agent Powell reported that PETERSEN reached in his bra and provided a paraphernalia pipe, two syringe needles and a small bag filled with a white substance. PETERSEN stated it was "dope". A NIK test was conducted on site and the results were positive for methamphetamine. The items were confiscated and booked into evidence. PETERSEN was searched pursuant to his arrest on the warrant as well as pursuant to AP&P's authority to search based on the reasonable suspicion of his violations of the terms of his probation. Agent Powell

also reported the PETERSEN had the SUBJECT CELLPHONE, with internet access in his possession that was not reported on the Sex Offender Registry.

30. In a cursory review of the phone by AP&P agents pursuant to AP&P search authority identified several messaging and social media applications, several email accounts including e81072990@gmail.com, mapritchet@gmail.com, edenpetersen40@gmail.com, and springtimerox@hotmail.com, images pertaining to "Adult Baby/Diaper Lover," and images of toddlers in diapers.

C. PETERSEN Continued to Access Child Pornography via the Internet During Probation

31. I submitted a request to NCMEC for a CyberTip technical analysis of several online identifiers known to be associated with PETERSEN. The resulting report identified 18 CyberTips, all submitted by Google LLC and associated to the identifiers known to be used by PETERSEN. Seven of the listed CyberTips were distributed to the Utah Internet Crimes Against Children (ICAC) Task Force prior or during the Utah AG's Office investigation, while 11 of them were received and submitted to NCMEC by Google LLC after PETERSEN's arrest by the AG's Office, indicating that PETERSEN's accounts continued to distribute, posses, and receive child pornography as identified and reported to NCMEC by Google LLC, well after his arrest, conviction, and sentencing.

32. In the technical analysis, NCMEC advised CyberTip 141101919 appeared to be associated with PETERSEN's identifiers. The CyberTip, submitted by Google LLC, advises that the account belonging to Eden Petersen with the email address "springtimerox@gmail.com" last accessed the internet on December 6, 2022, at 15:35:00 UTC. According to Google LLC, of 18 files of interest, four appeared to be child pornography and another five appeared to be

unconfirmed child pornography by hash value match to known child pornography databases. This report further indicates that PETERSEN continued to distribute, posses, and receive child pornography.

33. I know that cellphones are portable, versatile devices used to send, store, and receive digital media files and messages via numerous email, messaging, social media, and other communication applications. There is probable cause to believe that the evidence described above is digital in nature. Based on my training and experience and the information set forth above, including the Background on Internet and CSAM (Child Pornography), Therefore, there is probable cause to believe that evidence that inculpates PETERSEN in or exculpates him from the SUBJECT OFFENSES will be found in the SUBJECT CELLPHONE, as described in Attachment A.

SEARCH AND SEIZURE OF DIGITAL DATA

34. This application seeks permission to search for and seize evidence of the SUBJECT OFFENSES described above, including evidence of how computers, digital devices, and digital storage media were used, the purpose of their use, and who used them.

35. Based on my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that data in digital form can be stored on a variety of systems and storage devices, including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items.

36. I know from my training and experience, as well as from information found in

publicly available materials, that these digital devices offer their users the ability to unlock the device via the use of a fingerprint, thumbprint, or facial recognition in lieu of a numeric or alphanumeric passcode or password. These features are commonly referred to as biometric authentication and their availability is dependent on the model of the device as well as the operating system on the device. If a user enables biometric authentication on a digital device, he or she can register fingerprints, or his or her face, to unlock that device.

37. In some circumstances, biometric authentication cannot be used to unlock a device, and a passcode or password must be used instead. These circumstances include: (1) the device has been turned off or restarted; (2) the device has received a remote lock command; (3) too many unsuccessful attempts to unlock the device via biometric authentication are made; (4) too many hours have passed since the last time the device was unlocked; and (5) the device has not been unlocked via biometric authentication for a period of time and the passcode or password has not been entered for a certain amount of time. Thus, when law enforcement encounters a locked digital device, the opportunity to unlock the device via biometric authentication exists only for a short time.

38. The passcode or password that would unlock the SUBJECT CELLPHONE is not known to law enforcement. Thus, it is necessary to press the fingers of PETERSEN to the SUBJECT CELLPHONE's sensor, or hold the phone up to PETERSEN's face, in an attempt to unlock the devices for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device via biometric authentication is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant. I therefore request that the Court authorize law

enforcement officers to press the fingers, including thumbs, of PETERSEN to the fingerprint sensor of the SUBJECT CELLPHONE, or to hold the device equipped with facial recognition authentication up to PETERSEN's face, to unlock the device and thereby allow investigators to search the contents as authorized by this warrant.

FORENSIC IMAGING OF DATA STORAGE DEVICES

39. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant. I also know that during a search of premises it is not always possible to create a forensic image of or search digital devices or media for data for various reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. Because there are so many different types of digital devices and software in use today, it is difficult to anticipate all the necessary technical manuals, specialized equipment, and specific expertise necessary to conduct a thorough search of the media to ensure that the data will be preserved and evaluated in a useful manner.

b. Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data not readily apparent to the casual user. The recovery of such data may require the use of special software and procedures, such as those used in a law enforcement laboratory.

c. The volume of data stored on many digital devices is typically so large that it is generally highly impractical to search for data during the execution of a physical search of

premises. Storage devices capable of storing 500 gigabytes to several terabytes of data are now commonplace in desktop computers. It can take several hours, or even days, to image a single hard drive; the larger the drive, the longer it takes. Depending upon the number and size of the devices, the length of time that agents must remain onsite to image and examine digital devices can make doing an on-site search impractical.

LABORATORY SETTING MAY BE ESSENTIAL FOR COMPLETE AND ACCURATE ANALYSIS OF DATA

40. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, may be essential to conduct a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

41. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual.

Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

42. *Latent Data*: Searching digital devices can require the use of precise scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's operating system may keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

43. *Contextual Data*:

a. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, can indicate the identity of the user of the

digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software, may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

SEARCH OF SUBJECT CELLHONE

44. As described above and in **Attachment B**, this application seeks permission to search the SUBJECT CELLPHONE for child pornography in whatever form it is found. The warrant applied for would authorize the seizure of electronically stored information or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

45. As further described in **Attachment B**, this application seeks permission to locate

not only digital files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the SUBJECT CELLPHONE was used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be in the SUBJECT CELLPHONE.

46. Law enforcement personnel will examine the SUBJECT CELLPHONE to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in **Attachment B**. To the extent law enforcement personnel discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

47. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

48. The SUBJECT CELLPHONE was retained in AP&P Region 3 secure evidence storage. On January 8, 2024, U. S. Magistrate Judge Jared C. Bennett signed a District of Utah search warrant for the SUBJECT CELLPHONE. Due to several delays in retrieving the SUBJECT CELLPHONE for forensic analysis the warrant was not able to be executed within 14 days. As such, this warrant application is being resubmitted.

RETENTION OF IMAGE

49. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be

used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

CONCLUSION

50. Based upon the foregoing, I have probable cause to believe that Kevin PETERSEN committed the SUBJECT OFFENSES and that contraband and evidence, fruits, and instrumentalities of those violations, as described in Attachment B, will be located at the SUBJECT CELLPHONE, as described in Attachment A.

/s/ JEFFREY M. CHMIELEWSKI
Special Agent
Homeland Security Investigations

Sworn to before me telephonically or by other reliable means pursuant to Fed. R. Crim. P. 4.1 at 1:45 PM am/pm on March 1st, 2024.

HONORABLE Cecilia M. Romero
United States Magistrate Judge

ATTACHMENT A

(Property to be Searched)

"Notwithstanding Title 18, United States Code, Section 2252A, Meta Platforms, Inc. shall disclose responsive data, if any, by delivering encrypted files through Facebook's law enforcement portal."

A black TCL Stylus 5G T779W cellphone (bearing International Mobile Equipment Identity (IMEI) 016099001432453).

ATTACHMENT B

(Particular Things to be Seized)

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of Coercion and Enticement in violation of 18 U.S.C. § 2422(b) (online enticement of a minor), 18 U.S.C. §§ 2252(a)(1) and (2) and 2252A(a)(2) (Transportation/Receipt/Distribution of Child Pornography), and 18 U.S.C. §§ 2252(a)(4) and 2252A(a)(5)(B) (Possession of Child Pornography), and are contained in the SUBJECT CELLPHONE as described in **Attachment A**:

1. All CSAM, including:

    a. Child pornography, as defined in 18 U.S.C. § 2256(8),

    b. Visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

    c. Child erotica;

    d. Records, information, and items relating to a sexual interest in children;

2. Evidence of who used, owned, or controlled the SUBJECT CELLPHONE] at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

3. Evidence of the presence or absence of software that would allow others to control the

SUBJECT CELLPHONE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

a. Evidence of the lack of such malicious software;

b. Evidence indicating how and when the SUBJECT CELLPHONE were accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the SUBJECT CELLPHONE user;

c. Evidence indicating the SUBJECT CELLPHONE user's knowledge and/or intent as it relates to the crime(s) under investigation;

d. Evidence of the attachment to the SUBJECT CELLPHONE of other storage devices or similar containers for electronic evidence;

e. Evidence of programs (and associated data) that are designed to eliminate data from the SUBJECT CELLPHONE;

f. Evidence of the times the SUBJECT CELLPHONE was used;

g. Records of or information about Internet Protocol addresses accessed by the SUBJECT CELLPHONE;

h. Records of or information about the SUBJECT CELLPHONE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search

engine, and records of user-typed web addresses;

i. Contextual information necessary to understand the evidence described in this attachment;

j. Records and information tending to identify or locate any children depicted in child pornography or suspected of being sexually exploited in any way;

k. Records and information relating to the sexual exploitation of children, including correspondence and communications between messaging platform users;

During the execution of the search of the SUBJECT CELLPHONE described in **Attachment A**, law enforcement personnel are also specifically authorized to compel PETERSEN to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of the SUBJECT CELLPHONE.

This warrant does not authorize law enforcement personnel to compel from PETERSEN the password or any other means that may be used to unlock or access the SUBJECT CELLPHONE, as described in the preceding paragraph.